Policy for

# GDPR Policy:
## Information Security Policy 23/24

## Document Control

| | | | |
|---|---|---|---|
| **Confidentiality Notice** | This policy document has been approved by the Governing Body of St Modwen's Catholic Primary School and is intended for internal and/or external publication. Where the document is identified for internal use the policy information may not be shared with external agencies or parents without the prior agreement of the Headteacher or authorizing committee. | | |
| **Document Details** | **Classification:** | Premies, Health and Safety Committee | |
| | **Policy Source:** | John Walker (Data Protection Officer) May 2023 Version | |
| | **Organisation:** | St Modwen's Catholic Primary School | |
| | **Documents reference:** | Policy number: STM56 | |
| | **Current Version Number:** | V1(10 pages) | |
| | **Current Document Approved by: (Committee)** | PH&S | |
| | **Date Approved:** | Autumn 2 Term 2023 | |
| | **Statutory Policy** | Yes | |
| | **Internal/External Policy (published on website)** | External – Publish on website | |
| | **Schedule Review:** | **Next Review date:** | **Review cycle** |
| | | Autumn Term 2 2024 | Annually |

| **Version Control Document revision and Approval History** | **Version** | **Date** | **Version created by:** | **Version approved by:** | **Comments** |
|---|---|---|---|---|---|
| | V1 | 7.11.2023 | School | PH&S | Revised August 2023 – John Walker Policy 12.5.2023 Amends – related policy links |
| | | | | | |

**Contents**

# Information Security Policy

## 1. Introduction

Information security is everyone's responsibility. Personal and sensitive data is used, stored, shared, edited and deleted each day.

This policy explains staff responsibilities that are already in contracts of employment and reflects statutory obligations.

Details of how personal data is used is contained within privacy notices. The data protection policy sets out how the school's statutory obligations are managed.
The policy applies to all school staff which includes governors, agency staff, contractors, work experience students and volunteers when handling personal data.

## 2. Information security breach

Information security breaches can happen in a number of different ways.
Examples include:

- sending a confidential email to the wrong recipient
- letters sent to the wrong address with health and SEN data included
- overheard conversations about a member of staff's health
- an unencrypted laptop stolen after being left in a car
- hacking of school systems
- leaving confidential documents containing personal data in a car that was stolen

These would all need to be reported to the school data compliance officer. Anything which a staff member becomes aware of even if they are not directly involved in needs to be reported. For example, if they know that document storage rooms are sometimes left unlocked at weekends.

The sooner the breach is notified to the right person, the sooner and more effectively it can be managed.

In certain situations, it is necessary to report a breach to the Information Commissioner's Office (ICO), the data protection regulator, and notify those whose information has been compromised within strict timescales. This is another reason why it is vital breaches are reported immediately.

## 3. Privacy on a day-to-day basis

Staff must be aware of data protection and privacy whenever they handle personal and sensitive data.

## 4. Sensitive personal data

Data protection is about looking after information about individuals. Even something as simpleas a person's name or their attendance record is personal data. However, some personal data is more sensitive. This is called **sensitive personal data** in this and the data protection policy. Greater care about how that data is used is required.
Sensitive personal data includes:

- safeguarding and child protection matters
- serious or confidential physical or mental health conditions
- special education needs (SEN) information
- details of serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved
- financial information about parents/carers and staff
- racial or ethnic origin

- political opinion
- religious beliefs or beliefs of a similar nature
- trade union membership
- genetic information
- sexual life or orientation
- actual or alleged criminal activity
- biometric information (e.g. fingerprints used for cashless catering)

## 5. Minimising the amount of personal data held

Restricting the amount of personal data, we hold on an individual is needed to help keep the personal data safe. You should never delete personal data unless you are sure you are allowed to do so. If you would like guidance on when to delete certain types of information please speak to the ICT Technician/Headteacher.

## 6. Basic IT expectations

**LOCK COMPUTER SCREENS:** A staff member's computer screen should be locked when it is not in use, even if they are only away from the computer for a short period of time. To lock a computer screen, press the "Windows" key followed by the "L" key.
If staff are not sure how to do this speak to a member of the IT department.

**BE FAMILIAR WITH THE TECH:** Staff should make sure that they familiarise themself with any software or hardware that they use. In particular, they need to understand what the software is supposed to be used for and any risks.
For example:

- electronic registers – set to the correct view so students cannot see personal data of classmates
- virtual classrooms – be careful that confidential information is not uploaded for students to access
- shared drives – ensure you know where to store information containing sensitive personal data

**HARDWARE AND SOFTWARE NOT PROVIDED BY ST MODEWN'S CATHOLIC PRIMARY SCHOOL:** Staff must not use, download, or install anysoftware, app, programme, or service without permission from the IT Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to IT systems without permission.

**PRIVATE CLOUD STORAGE:** Staff must not use private cloud storage or file sharing accounts tostore or share school documents.

**PORTABLE MEDIA DEVICES:** The use of portable media devices (such as USB drives) is not allowed unless those devices have been given to staff by the school andstaff have received training on how to use those devices securely. The IT Department will protect any portable media device given to you with encryption.

**IT EQUIPMENT:** If staff are given IT equipment to use (this includes laptops, printers and phones) staff must make sure that this is recorded on IT equipment asset register. IT equipment must always be returned to the IT Department even if you thinkthat it is broken and will no longer work, and the asset register updated accordingly.

## 7. Passwords

Passwords should be long and difficult to guess. Staff should not choose a password which is so complex that it's difficult to remember without writing it down. Passwords should not be disclosed to anyone else.

Staff should not use a password which other people might guess or know, or be able to findout, such as their address or birthday.

Staff must not use a password which is used for another account. For example, staff must not use a password used for their private email address or online services for any school account.

Passwords (and any other security credential staff are issued with such as a key fob or USBdrive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

## 8. Emails

When sending emails staff must take care and check to ensure that the recipients are correct.

Sending an email to multiple recipients, staff must be sure to check that they are using the correct 'To:' 'CC:' or 'BCC:' function.

If the email contains any personal data then staff should ask themselves is this the best communication method. Sometimes it is unavoidable so staff should ensure the email is sufficiently encrypted and ask an authorised staff member to check the email addresses have been entered accurately. When sending personal data over email, staff should consider inputting the information into an attachable document which is password protected.

Staff must not use a private email address for any school related work. A school email address must only be used. This also applied to governors/trustees.

## 9. Paper files

**KEEP UNDER LOCK AND KEY:** Staff must ensure that papers which contain personal data arekept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

If the papers contain critical personal data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below. Information held in paperform must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (DSL) room.

| Cabinet | Location | Access |
|---|---|---|
| **Child protection** | School Business Manager Office – Locked Filing Cabinet | Headteacher and DSL |
| **Financial information** | School Business Manager Office – Locked Filing Cabinet | Headteacher/School Business Manager and authorised personnel e.g. Office Manager, Deputy Headteacher, School Business Team |
| **Health information** | Pupil Accident Books – Classrooms/Concourse/Medical Room<br>Master IHCP's, PEEP's, Allergens - School Business Manager Office – Locked Filing Cabinet<br>EHCP's Deputy Headteacher/SENDCO Office | Headteacher/Deputy Headteacher/SENDCO, School Business Manage, and authorised personnel e.g. SENDCO, Inclusion Manager, Attendance & Admissions Manager, Office Manager, School Business Team |

**DISPOSAL:** Paper records containing personal data should be disposed of securely shredding the material and disposing the paper waste in recycling. Personal data should never be placed in the general waste.

**PRINTING:** When printing documents, staff must collect everything from the printer straight away, otherwise there is a risk that confidential information being read or picked up by someone else. If you see anything left by the printer which contains personal data then you must hand it in to the office.

**PUT PAPERS AWAY:** Staff should always keep a tidy desk and put papers away when they are no longer needed.

**POST:** Staff also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If staff need to send something in the post that is confidential, consider asking the IT team to put it in on an encrypted memory stick or arrange for it to be sent by courier.

## 10. Working off-site

Staff might need to take personal data off-site for various reasons such as remote working or supervising a school trip. This does not breach data protection law if the appropriate safeguards are in place to protect personal data.

For school trips, the trip supervisor should decide what information needs to be taken and who will be responsible for looking after it. Any personal data taken off-site must be returned back to school.
When a staff member works from home, they should check with School Business Manager/Office Manager whether any additional arrangements need to be put in place to ensure the security of data.

**ONLY TAKE THE MINIMUM:** When working away from school staff must only take theminimum amount of information with them. For example, if only eight out of a class of twenty pupils are attending the trip,then the teacher should only take the information about the eight pupils.

**WORKING ON THE MOVE:** Staff must not work on documents containing personal data whilst travelling if there is a risk of unauthorised disclosure. For example, if working on a laptop on a train, the individual should ensure that no one else can see the laptop screen and they should not leave any device unattended where there is a risk of theft.

**PAPER RECORDS:** If staff need to take hard copy records with them then they should make sure that they are kept secure.
For example:

- documents should be kept in a locked case
- information should be kept with them at all times
- the individual must keep the documents out of plain sight
- if the individual has a choice between leaving documents in a vehicle and taking them with them (e.g. to a meeting) then they should be taken with them

**PUBLIC WI-FI:** Staff must not use public Wi-Fi to connect to the internet. If working in a public café, the individual should use their 4G or 5G.

## 11. Using personal devices to access school work

Staff may only use their personal device (such as your laptop or smartphone) for school work if you have been given permission by the Headteacher. Please note you will also need to complete and sign an Acceptable use of Own Devices Declaration, this will need to be reviewed and signed annually.

Even if they have been given permission to do so, then before using their own device they must speak to the IT team so that they can configure the device.

Appropriate security measures should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

**DEFAULT PASSWORDS:** If a personal device for school work came with a default password then this password should be changed immediately.

**SENDING OR SAVING DOCUMENTS TO YOUR PERSONAL DEVICES:** Documents containing personal data (including photographs and videos) should not be sent to or saved to personal device. This is because anything you save to your computer, tablet or mobile phone will not be protected by security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer.

**FRIENDS AND FAMILY:** Staff must take steps to ensure that others who use their device) cannot access anything school related information. Staff must make sure that the device is not configured in a way that would allow someone else access to school related documents and information – if they are unsure about this then they need to contact the IT department who can assist with this.

**WHEN YOU STOP USING YOUR DEVICE FOR SCHOOL WORK:** If the individual stops using your device for school work, all documents including emails and software applications provided by the school must be removed from the device.

## 12. Breach of this policy

Any breach of this policy will be taken seriously and may result in disciplinary action.

A member of staff who deliberately or recklessly obtains or discloses personal data held by [school name] without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

This policy does not form part of any employee's contract of employment.

We reserve the right to change this policy at any time. Where appropriate, we will notifystaff of those changes by email.

## 13. GDPR related policies

| | Review Date |
|---|---|
| 01 Data Protection Policy | September 2024 |
| 02 Breach and Non-Compliance Policy | September 2024 |
| 03 Confidentiality Policy and Confidential Agreements | September 2024 |
| 04 CCTV Policy | September 2024 |
| 05 Workforce Acceptable use Policy | September 2024 |
| 06 Freedom of Information Policy | September 2024 |
| 07 Document and Data Retention Policy | September 2024 |

| | |
|---|---|
| 08 Privacy Notices:<br>• Pupils Data<br>• School Trips<br>• Staff Workforce<br>• Governors<br>• Job Applicants<br>• PTA<br>• External School Photographer | September 2024 |
| 09 GDPR Workforce and Governor Training/CPD<br>• GDPR Guidelines for staff | September 2024 |
| 10 GDPR Checks, Compliance and Audit Toolkit (GoGDPR) | September 2024 |
| 11 GDPR Subject Access Request Management and Procedures | September 2024 |
| 12 GDPR My rights a guide for data subjects | September 2024 |
| 13 GDPR Home School Communication Charter | September 2024 |
| 14 GDPR Information Security Protocol | September 2024 |
| 15 Cyber Response Plan | September 2024 |
| | |

# Appendix 1 - Protocols for the use of phone in school

## RESPONSIBILITY

Mobile phones brought into school are entirely at the staff member, pupil's, parent's or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any mobile phone.

The school reserves the right to search the content of any mobile phone on the school premises where there is reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles may be searched at any time as part of routine monitoring.

The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; except where it has been explicitly agreed otherwise by the headteacher.

All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at anytime if it is to be deemed necessary.

Mobile phones are not permitted to be used in certain areas within the school premises, e.g. changing rooms and toilets.

## STAFF

All staff mobile phones must be secured in the locked cabinets provided or kept in a secure place and not used during lesson/formal school time.

Staff members may use their phones during school break times in certain areas.

Mobile phones will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

## STAFF USE OF MOBILE PHONES

Staff are not permitted to use their own mobile phones for contacting pupils, parents/carers or their families within or outside of the setting in a professional capacity.

Staff will be issued with a school phone where contact with pupils, parents or carers is required.

Staff will also be issued with a school phone whilst on educational off-site visits.Alternatively, staff may have permission from the headteacher or the trip supervisor to bring their own mobile phones on trips to be used strictly for communication with the school or for emergency situations.

Bluetooth communication should be 'hidden' or switched off. They will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

If members of staff have an educational reason to allow pupils to use mobile phones or aas part of an educational activity, then it will only take place whenapproved by the senior leadership team.

Staff must not use their personal mobile phone to take photos or videos of pupils and will only use work-provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action may be taken.

Where staff members are required to use a mobile phone for school duties, for instance in case of

emergency during off-site activities, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school owned device, they should use their own device and hide their own mobile number for confidentiality purposes.

## VISITORS

All visitors are requested to keep their phones on silent.

## PARENTS AND PUPILS

Where parents or pupils need to contact each other during the school day, they should do so through the school's telephone.

## PUPILS' USE OF PERSONAL DEVICES

The school strongly advises that pupil mobile phones should not be brought into school/academy.

The school accepts that there may be particular circumstances in which a parent wishes theirchild to have a mobile phone for their own safety.

If a pupil breaches the school policy then the phone will be confiscated and will beheld in a securely in the school office. Mobile phones will be released to parents or carers in accordance with the school policy.

Mobile phones are prohibited to be taken into any examination. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.

If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

## DIGITAL IMAGES AND VIDEOS

In St Modwen's Catholic Primary School:

- consent is sought from parents/carers for use of images and videos involving their child as part of the Application pack when their son/daughter joins the school
- pupils are not identified in online photographic materials or include the full names of the pupil
- staff confirm that they have read and understood this policy
- any photos used on the school website or prospectus, parents/carers will be asked to provide consent
- pupils are taught about how images can be manipulated in their e-safety education programme
- pupils are advised to be very careful about placing any personal photos on any 'social' online network space
- pupils are taught that they should not post images or videos of others without their permissions.